Federal Transition Framework
Catalog of Cross Agency Initiatives

Pilot Version

June 2006

Revision History

Date	Version	Approver	Summary of changes
June 2006	Pilot	Dick Burk	Initial version

Table of Contents

1 Introduction

1.1 OVERVIEW

The Federal Transition Framework (FTF) provides clear and consistent information to describe government-wide IT policy objectives and cross-agency initiatives.

The FTF does not create IT policy. It provides a simple structure to organize and publish existing information to:

- Enhance the quality and consistency of information on cross-agency initiatives
- Increase the level and speed of adoption of cross-agency initiatives
- Improve the overall effectiveness and efficiency of IT investments and programs related to cross-agency initiatives.

1.2 ABOUT THE FTF PACKAGE

Three documents are provided to describe the content and structure of the Federal Transition Framework and how it should be used:

- **FTF Usage Guide**: Provides guidance to agency decision-makers and cross-agency stakeholders on how to apply and extend the FTF. This is the first document to read when starting to learn about the FTF and how it should be used.
- **FTF Catalog**: Provides a written description and information references for cross-agency initiatives included in the FTF.
- **FTF Metamodel Reference**: Provides information on the internal structure of the FTF. This document is provided as a technical reference for architects.

1.3 ABOUT THIS DOCUMENT

This document is a catalog of architectural content produced by selected Federal cross-agency initiatives. Subsequent releases of the FTF Catalog will incorporate content from additional cross-agency initiatives, including OMB Line of Business initiatives, E-Government initiatives and other initiatives that span multiple Federal agencies.

The content for each initiative includes elements such as common business processes, legislative mandates, information exchange packages, shared service components, common technology standards and others. This content is structured according to the FTF metamodel, which is documented in the FTF Metamodel Reference. The content of the catalog is designed to be incorporated into agency target architectures and transition strategies.

1.4 FTF CONTACT INFORMATION

Email: fea@omb.eop.gov

2 FTF Catalog

2.1 THE IPV6 TRANSITION CROSS-AGENCY INITIATIVE

- **Initiative**
  - **Name**: IPv6 Transition Cross-Agency Initiative
    Description: The IPv6 cross-agency initiative describes all common architecture elements pertaining to the implementation of Internet Protocol Version 6 (IPv6). OMB Memorandum 05-22 mandates all federal agencies' infrastructure (network backbones) must be using IPv6, and agency networks must interface with this infrastructure, by June 30, 2008.
    Mandatory: Yes. Incorporation of IPv6 into agency enterprise architectures is mandated by OMB Memorandum 05-22.
    Applicable Agencies: All federal agencies. No exemptions have been granted.
    Managing Partner: OMB

- **Communities of Interest**
  - Federal COIs
    - **Name**: CIO Council Architecture and Infrastructure Committee: IPv6 Working Group.
    - **Description**: This working group is responsible for identifying best practices associated with IPv6 implementation and issuing advisory guidance to federal agencies
      URL: <TBD>
      Contact Name: John McManus, Deputy CIO, CTO, NASA
      Contact Email: jmcmanus@nasa.gov
  - Other COIs
    - None

- **Guidance**
  - OMB Guidance
    - **Name**: OMB Memorandum 05-22, "Transition Planning for Internet Protocol Version 6"
      Description: This Memorandum describes both the compliance requirements and the timetable for IPv6 implementation within agency network backbones.
      Date: August 2, 2005
      URL: http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf
  - CIO Council Guidance
    - **Name**: Integrating IPv6 into Agency EA Planning
      Description: Chapter 1 of CIOC IPv6 guidance; describes best practices for integrating IPv6 transition planning into agency enterprise architecture activities
      URL:
      http://www.cio.gov/documents/Integrating_IPv6_into_Agency_EA_Planning.doc

- **Name**: IPv6 Transition Planning – Transition Elements
  Description: Chapter 2 of CIOC IPv6 guidance; describes specific elements to be incorporated into the agency's IPv6 Transition Plan and provides an overview of IPv6 features, benefits and implementation challenges
  URL: <TBD>
- **Name**: IPv6 Governance
  Description: Chapter 3 of CIOC IPv6 guidance; describes best practices for governing the IPv6 transition within the agency, including roles and responsibilities, relevant federal regulations and related communities of interest.
  URL: <TBD>
- **Name**: Federal Government Guide to IPv6 Acquisition and Procurement
  Description: Chapter 4 of CIOC IPv6 guidance; provides guidance on complying with relevant FAR clauses for procurement and an explanation of the federal IPv6 technical standards
  URL: <TBD>

▪ Other Approved Guidance (e.g. NIST, GSA, etc.)

- TBD (FAR Guidance, NIST standards)

o **Performance and Strategy Layer**

▪ Mandates

- **Name**: OMB Memorandum 05-22, "Transition Planning for Internet Protocol Version 6"
  Description: This Memorandum describes both the compliance requirements and the timetable for IPv6 implementation within agency backbones.
  URL: http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf
  Mandate Type: OMB Memoranda

▪ Requirements

- **Name**: IPv6 Capability within Agency Network Backbone
  Description: The agency's network backbone must either be operating a dual stack network core or to be operating in a pure IPv6 mode (i.e., configured to successfully carry operational IPv6 traffic) by June 30, 2008. Agency networks are required to interface with the upgraded network backbone, while maintaining continuity of operations and security during and after transition. Agencies must verify this capability through testing activities.
  Requirement Source: OMB Memorandum 05-22

▪ Outcomes

- Agencies must be able to transmit both IPv4 and IPv6 data from the Internet and external peers to the LAN[1].
- Agencies must be able to transmit both IPv4 and IPv6 data from the LAN out to the Internet and external peers.
- Agencies must be able to transmit both IPv4 and IPv6 data from the LAN to another LAN (or another node on the same LAN).

[1] Agencies are required to transmit IPv4 and IPv6 data to the point of LAN demarcation. This is the hardware device serving the LAN, such as a router or switch.

        - Agencies must maintain continuity of operations and security during and after adoption of IPv6 technology into the network.
    - Related PRM Measurement Categories
        - Information and Technology Management
    - Related PRM Measurement Groupings
        - IT Infrastructure Maintenance
        - IT Security

- **Business Layer**
    - Federal Initiatives/Lines of Business (e.g. IT Management)
        - None
    - Common Business Processes
        - **Name**: IPv6 Address Space Acquisition
          Description: All agencies must submit requests for IPv6 address space directly to American Registry for Internet Numbers (ARIN) or their Internet Service Provider (ISP). The National Telecommunication and Information Administration (NTIA) will be available to assist Federal government agencies with these requests.
          URL: http://www.arin.net/, http://www.ntia.doc.gov/
          Process Owner: National Telecommunications and Information Administration (NTIA), Cathy Handley, chandley@ntia.doc.gov
    - Related BRM Subfunctions
        - IT Infrastructure Maintenance (Information and Technology Management)
        - IT Security (Information and Technology Management)
    - Related Requirements
        - IPv6 Capability Within Agency Network Backbone

- **Data Layer**
    - Taxonomies
        - None
    - Topics
        - None
    - Data Assets
        - None
    - Query Points
        - None
    - Exchange Packages
        - None
    - Entities
        - None
    - Related Business Processes
        - None

- **Service Component Layer**
    - Shared Services
        - None
    - Shared Components

- None
- Component Repositories
  - None
- Related SRM Service Components
  - Network Management
  - Computers/Automation Management
  - Encryption
- Related Business Processes
  - IPv6 Address Space Acquisition

- **Technology Layer**
  - Approved Federal Technology Standards
    - **Name**: Federal Acquisition Regulations (FAR) IPv6 amendment
      Description: Details of IPv6 FAR amendment will be released to agencies after FAR council has finalized language.
      URL: <TBD>
  - SmartBUY Licensing Agreements
    - None
  - Related TRM Service Standards
    - Internet Protocol (Service Transport)
    - IPSec (Service Transport)
  - Related Shared Components
    - None

2.2 IT INFRASTRUCTURE OPTIMIZATION

- **Initiative**
  - **Name**: IT Infrastructure Optimization
    Description: The IT Infrastructure Optimization cross-agency initiative responsible for identifying best practices for information technology infrastructure to be executed and leveraged across agencies.
    Mandatory: No. This Line of Business has currently developed a Reference Architecture described below, which agencies may consult for informational purposes. Agencies are not required to incorporate this Initiative into their target architectures at this time. This initiative is expected to become mandatory for inclusion into agency target architectures at a later date.
    Applicable Agencies: All federal agencies.
    Managing Partner: General Services Administration (GSA)

- **Communities of Interest**
  - Federal COIs
    - **Name**: IT Infrastructure Optimization Task Force
      Description: This cross-agency task force is responsible for identifying best practices associated with IPv6 implementation and issuing advisory guidance to federal agencies
      URL: http://www.core.gov
      Contact Name: Tom Brady
      Contact Email: tom.brady@gsa.gov
  - Other COIs
    - None

- **Guidance**
  - OMB Guidance
    - TBD
  - CIO Council Guidance
    - TBD

- **Performance and Strategy Layer**
  - Mandates
    - TBD
  - Requirements
    - TBD
  - Outcomes
    - TBD
  - Related PRM Measurement Categories
    - Internal Risk Management and Mitigation
      - Contingency Planning
      - Continuity of Operations
      - Service Recovery
    - Management of Government Resources

        - Infrastructure Maintenance
    - Financial
        - Overall Costs
        - Licensing Costs
        - Support Costs
        - Operations and Maintenance Costs
        - Training and User Costs
    - Quality
        - Functionality
        - IT Composition
        - Compliance and Deviations
    - Efficiency
        - Response Time
        - Interoperability
        - Accessibility
        - Load Levels
        - Improvement
    - Information and Data
        - Data Storage
    - Reliability and Availability
        - Availability
        - Reliability
    - Effectiveness
        - User Satisfaction
        - User Requirements
        - IT Contribution to Process, Customer or Mission

- **Business Layer**
    - Federal Initiatives/Lines of Business (e.g. IT Management)
        - IT Infrastructure Line of Business
    - Common Business Processes
        - **Name**: Help Desk
          Description: A help desk is an information and assistance resource troubleshooting problems with computers and other information technology products.
          URL: <TBD>
          Process Owner: GSA
        - **Name**: Seat Management
          Description: Desktop/seat management typically refers to the acquisition, deployment, and ongoing support of the technology associated with the desktop computing environment.
          URL: <TBD>
          Process Owner: GSA
        - **Name**: Data Center
          Description: A data center is usually maintained by an organization for the purpose of handling the data necessary for its operations.

URL: <TBD>
Process Owner: GSA

- **Name**: Telecommunications
  Description: Telecommunications (telecom) refers to communication over long distances. Telecom typically covers all forms of distance and/or conversion of the original communications, including radio, telegraphy, television, telephony, data communication and computer networking.
  URL: <TBD>
  Process Owner: GSA
- **Name**: Data Network
  Description: A data network can be described as the hardware, software, and communication services allowing any two computers or other devices to exchange data between them.
  URL: <TBD>
  Process Owner: GSA

- Related BRM Subfunctions
  - Internal Risk Management and Mitigation
    - Contingency Planning
    - Continuity of Operations
    - Service Recovery
  - Information and Technology Management
    - IT Infrastructure Maintenance
- Related Requirements
  - TBD

o **Data Layer**

- Taxonomies
  - None
- Topics
  - None
- Data Assets
  - None
- Query Points
  - None
- Exchange Packages
  - None
- Entities
  - None
- Related Business Processes
  - None

o **Service Component Layer**

- Shared Services
  - TBD
- Shared Components
  - TBD
- Component Repositories

- TBD
- Related SRM Service Components
  - Management of Process
    - Configuration Management
    - Quality Management
    - Risk Management
  - Organizational Management
    - Network Management
  - Data Management
    - Data Recovery
  - Assets/Materials Management
    - Facilities Management
    - Computers/Automation Management
  - Communication
    - Event/News Management
    - Computer/Telephony Integration
    - Voice Communications
  - Systems Management
    - License Management
    - Remote Systems Control
    - System Resource Monitoring
    - Software Distribution
    - Issue Tracking
- Related Business Processes
  - TBD

o **Technology Layer**

- Approved Federal Technology Standards
  - **TBD**
- SmartBUY Licensing Agreements
  - TBD
- Related TRM Service Standards
  - Access Channels
    - Web Browser
    - Collaboration/Communication
  - Delivery Channels
    - Internet
    - Intranet
    - Extranet
    - Virtual Private Network (VPN)
  - Service Requirements
    - Hosting
  - Service Transport
    - Supporting Network Services
    - Service Transport
  - Support Platforms
    - Platform Independent

        - Platform Dependent
    - Delivery Servers
        - Web Servers
    - Database/Storage
        - Storage
    - Hardware/Infrastructure
        - Servers/Computers
        - Embedded Technology Devices
        - Peripherals
        - Wide Area Network (WAN)
        - Local Area Network (LAN)
        - Network Devices/Standards
- Related Shared Components
    - TBD

2.3 E-AUTHENTICATION

- **Description**
  - **Name**: E-Authentication Service Component
    Description: E-Authentication is providing the standards, framework, governance and services necessary for the Federal Government to accept all levels of secure identity verification, simplifying business, public & government access to online services in a cost-effective manner.
    Mandatory: Yes.
    Applicable Agencies: All federal agencies implementing public-facing websites requiring authentication.
    Managing Partner: General Services Administration (GSA)

- **Communities of Interest**
  - Federal COIs
    - **Name**: CIO Council E-Authentication Website
      Description: The Chief Information Officers Council is the principal interagency forum to assist CIOs in realizing their mandates to ensure the rapid and effective implementation of information management and information technology (IM/IT) solutions within each agency and to create a more results-oriented, efficient, and citizen-centered Federal government.
      URL: http://www.cio.gov/eauthentication/
      Contact Name: Michel Kareis
      Contact Email: michel.kareis@gsa.gov
  - Other COIs
    - Information Systems Security Line of Business (ISSLOB) – the four common solutions currently addressed in the ISSLOB Line of Business do not directly affect the E-Authentication Initiative. When/if additional common solutions are identified in future years, the potential coordination/interaction with E-Authentication may need to be addressed.
    - Federal Agency CISOs
    - Federal Agency Web-enabled IT System Program/Project Managers
    - Federal Agency Privacy Officers
    - Federal E-Gov Initiatives
    - Potential Credential Service Providers (Government and Commercial)
    - Industry Identity Management community -- organizations dedicated to the field, such as OASIS, Liberty Alliance, etc

- **Guidance**
  - OMB Guidance
    - **Name**: OMB Memorandum 04-04, "E-Authentication Guidance for Federal Agencies
      Description: This document provides agencies with guidance on electronic authentication (e-authentication). The National Research Council report, "Who Goes There? Authentication Through the Lens of Privacy"[3] defines e-

authentication as the process of establishing confidence in user identities electronically presented to an information system. It defines individual authentication as the process of establishing an understood level of confidence an identifier refers to a specific individual.
URL: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

- CIO Council Guidance
  - **Name:** Certificate Lifecycle Methodology for E-Governance Certificate Authorities
    Description: This document describes the specific process established by the Federal Public Key Infrastructure Policy Authority (FPKIPA) for issuing and managing certificates from E-Government Certificate Authorities.
    URL:
    http://www.cio.gov/eauthentication/documents/EGCAmethodology.pdf
  - **Name:** E-Authentication Federation Legal Document Suite
    Description: This document includes: 1) E-Authentication Federation CSP Participation Agreement, 2) E-Authentication Federation Relying Party Participation Agreement, 3) E-Authentication Federation Interim Business Rules, 4) E-Authentication Federation Interim Operating Rules.
    URL: http://www.cio.gov/eauthentication/documents/LegalSuite.pdf
  - **Name**: E-Authentication Credential Assessment Suite
    Description: This document includes: 1) Guide to Preparing for a Credential Assessment, 2) Certificate Credential Assessment Profile, v2.0.0, 3) Password Credential Assessment Profile, v2.0.0, 4) Credential Assessment Framework, v2.0.0, 5) Entropy Spreadsheet, v2.0.0.
    URL: http://cio.gov/eauthentication/CredSuite.htm
  - **Name**: Electronic Risk and Requirements Assessment (E-RA)
    Description: This document includes: 1) E-Authentication E-RA Tool Activity Guide v1.5, 2) E-RA Tool.
    URL: http://cio.gov/eauthentication/era.htm
- Other Approved Guidance (e.g. NIST, GSA, etc.)
  - **Name**: NIST Special Publication 800-63, "Electronic Authentication Guideline"
    Description: This recommendation provides technical guidance to Federal agencies implementing electronic authentication. The recommendation covers remote authentication of users over open networks. It defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, authentication protocols and related assertions.
    URL: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf
  - **Name**: X. 509 Certificate Policy for E-Government Certification Authorities
    Description: This document defines a suite of policies applying to the management of the E-Governance Certification Authorities.
    URL: http://www.cio.gov/fpkipa/documents/EGovCA-CP.pdf
  - **Name**: E-Authentication Handbook for Federal Government Agencies
    Description: This handbook presents general guidelines to Government Agencies planning to participate or already participating in the E-Authentication Initiative (Initiative). The handbook provides a full life cycle

view of E-Authentication participation, so as to provide Agencies with complete Initiative perspective and guidance.
URL: http://www.cio.gov/eauthentication/documents/GOVhandbook.pdf

- **Performance and Strategy Layer**
  - Mandates
    - **Name**: OMB Memorandum 04-04, "E-Authentication Guidance for Federal Agencies
      Description: This document provides agencies with guidance on electronic authentication (e-authentication). The National Research Council report, "Who Goes There? Authentication Through the Lens of Privacy"[3] defines e-authentication as the process of establishing confidence in user identities electronically presented to an information system. It defines individual authentication as the process of establishing an understood level of confidence an identifier refers to a specific individual.
      URL: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
      Mandate Type: OMB Memorandum
    - **Name:** Privacy Act of 1974
      Description: The Privacy Act pertains to the E-Authentication Initiative for protection of authentication data from unauthorized disclosure or modification.
      URL: http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm
      Mandate Type: Act of Congress
    - **Name:** HSPD-12
      Description: Policy for a Common Identification Standard for Federal Employees and Contractors. This policy addresses similar issues as E-Authentication, but in a broader context.
      URL:http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html
      Mandate Type: Presidential Directive
    - **Name:** FIPS 200 "Minimum Security Requirements for Federal Information and Information Systems"
      Description: The E-Government Act (P.L. 107-347), passed by the one hundred and seventh Congress and signed into law by the President in December 2002, recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA), emphasizes the need for each federal agency to develop, document, and implement an enterprise-wide program to provide information security for the information and information systems that support the operations and assets of the agency including those provided or managed by another agency, contractor, or other source.
      URL: http:// csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf
      Mandate Type: NIST Standard
  - Requirements
    - Categorization of all existing transactions/systems requiring user authentication into one of the four assurance levels by Sep. 15, 2005

(specified in OMB Memorandum 04-04). The four assurance levels are also described in detail in NIST SP800-63.

- Privacy Impact Assessment (PIA) needs to be performed when E-Authentication technology is added to an information system that serves the public (E-Government Act of 2002 section 208). OMB guidance for implementing privacy provisions of the E-Gov Act is provided at http://www.whitehouse.gov/omb/memoranda/m03-22.html.
- Implement a level of authentication appropriate for the information system being accessed, using levels 1-4 defined in OMB and NIST guidance.
- Accept identity assertions from appropriate E-Authentication Federation-member third party credential service providers
- Agency authentication policy should align with OMB M-04-04, "E-Authentication Guidance for Federal Agencies"
- Agency Web-system development processes and procedures should build in step to engage with E-Authentication
- Business cases for Web-systems should include E-Authentication alignment

- Outcomes
  - Reduce the number of security weaknesses of federal information systems, resulting from inadequate authentication of user identity (provide appropriate level 1-4 authentication services for all information systems that require them).
  - Build trust in the information sharing infrastructure of the federal government by enabling stronger authentication for government to citizen (G2C), government to business (G2B), and government to government (G2G) transactions.
  - Reduction in government's overall identity management burden by elimination of proprietary credentialing systems.
  - Improved customer service to agency constituents, reducing the need for end users to create new user accounts for each online government service and simplifying the process of doing business with the government.
- Related PRM Measurement Categories
  - Information and Technology Management
- Related PRM Measurement Indicators
  - IT Security

o **Business Layer**

- Federal Initiatives/Lines of Business (e.g. IT Management)
  - Information and Technology Management
- Common Business Processes
  - Identity Authentication
  - Review and approval of trusted certification credential services
  - Review and approval of e-authentication technology providers
- Related BRM Subfunctions
  - IT Infrastructure Maintenance (Information and Technology Management)
  - IT Security (Information and Technology Management)
- Related Requirements

- Implement and manage E-authentication functionality for E-Government initiatives
- Provide a reusable E-authentication resource for agency information systems

- **Data Layer**
  - Taxonomies
    - Lists and descriptions of required data are included in the X.509 Certificate Policy Document at http://www.cio.gov/fpkipa/documents/EGovCA-CP.pdf
  - Topics
    - None
  - Data Assets
    - List of approved Trusted Credential Service Providers at http://www.cio.gov/eauthentication/documents/TCSPlist.pdf.
  - Query Points
    - Credential Service Providers http://www.cio.gov/eauthentication/documents/TCSPlist.pdf
  - Exchange Packages
    - e-Authentication Technical Suite (see Technology Layer below)
    - X.509 version 3 Certificate
  - Entities
    - None
  - Related Business Processes
    - Processes and policies regarding certificate data are included in the X.509 Certificate Policy Document at http://www.cio.gov/fpkipa/documents/EGovCA-CP.pdf

- **Service Component Layer**
  - Shared Services
    - **Name:** E-Authentication Interoperability Lab
      Description: The Lab tests software products, services, and Authentication Service Component (ASC) components for compliance to E-Authentication's Interface Specifications, which are a subset of industry standards. In addition, the Lab tests software products for interoperability with the approved software products that purport the same compliance.
      URL: http://www.cio.gov/eauthentication/IOLabAppWin.htm
  - Shared Components
    - **Name**: Approved E-Authentication Technology Provider List
      Description: List of approved e-authentication technology providers
      URL: http://cio.gov/eauthentication/documents/ApprovedProviders.htm.
    - **Name**: e-Authentication Service Component (ASC)
      Description: The E-Authentication Service Component is a common infrastructure for electronically authenticating the identity of users of Federal E-Government services Government wide. Using a common network, this infrastructure links identity suppliers (termed Credential Service Providers or CSPs) and identity consumers (termed Agency Applications or AAs) enabling participating CSPs and AAs to communicate

in a standardized way. Lists of approved E-Authentication Technology Providers and trusted credential providers are available on the E-Authentication website.
URL: http://www.cio.gov/eauthentication/

- Component Repositories
  - CORE.GOV
- Related SRM Service Components
  - Identification and Authentication (Security Management)
- Related Business Processes
  - Identity Authentication
  - Review and approval of trusted certification providers
  - Review and approval of e-authentication technology providers

o **Technology Layer**

- Approved Federal Technology Standards
  - **Name**: Security Access Markup Language (SAML)
    Description: An XML standard enabling the exchange of authentication and authorization information among business partners for Web services. E-Authentication has selected SAML version 1.0.
    URL: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
  - **Name**: x.509v3 Digital Certificates
    Description: X.509 is a standard defining a standard certificate format for public key certificates and certification validation.
    URL: http://www.ietf.org/html.charters/pkix-charter.html
  - **Name:** E-Authentication Technical Architecture
    Description: Set of documents providing the following: **1)** Description of the technical approach for the E-Authentication Initiative. The approach is based on architectural framework allowing multiple protocols and federation schemes to be supported over time, and is subject to periodic revision and update. **2)** Overview of the SAML 1.0 Artifact Profile in the E-Authentication Initiative. **3)** Interface specifications for the SAML Artifact Profile for use in with the E-Authentication Initiative. **4)** Specific requirements for path validation, path discovery, and auditing for PKI clients used in the federal PKI.
    URL: http://www.cio.gov/eauthentication/TechSuite.htm
- SmartBUY Licensing Agreements
  - None
- Related TRM Service Standards
  - Certificates/Digital Signature (Security)
- Related Shared Components
  - E-Authentication Service Component (ASC)